PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

Comments -- NBP Public Notice #2

~~Grid Net~~ Response to FCC Solicitation for Comments on The Implementation of Smart Grid Technology

GN Docket Nos. 09-47, 09-51, 09-137

1. **Suitability of communications technologies**. Smart Grid applications are being deployed using a variety of public and private communications networks. We seek to better understand which communications networks and technologies are suitable for various Smart Grid applications.
   a. What are the specific network requirements for each application in the grid (e.g., latency, bandwidth, reliability, coverage, other)? If these differ by applications, how do they differ? We welcome detailed Smart Grid network requirement analyses.

   RESPONSE: We view the Smart Grid as a series of interconnected, interoperable networks of control systems and asset-management tools, empowered by sensors, communication pathways and information tools – all designed to help utilities deliver energy more efficiently to customers. Smart Grid networks include (but are not limited to): substation automation, power distribution network monitoring & control, field operations communications, smart metering, and home area networks. Smart Grid networks must meet a range of demanding and immediate requirements: for security, coverage, functionality, reliability, performance, cost, and manageability (see table below). In addition, these networks must also offer architectures and technology roadmaps that extend well into the future, so this major utility investment can continue to support mission-critical operations into the next generation and beyond. A summary of differences in network requirements is as follows:

PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

Comments -- NBP Public Notice #2

Grid Net Response to FCC Solicitation for Comments on The Implementation of Smart Grid Technology

FILED/ACCEPTED
OCT - 2 2009
Federal Communications Commission
Office of the Secretary

GN Docket Nos. 09-47, 09-51, 09-137

1. **Suitability of communications technologies**. Smart Grid applications are being deployed using a variety of public and private communications networks. We seek to better understand which communications networks and technologies are suitable for various Smart Grid applications.
    a. What are the specific network requirements for each application in the grid (e.g., latency, bandwidth, reliability, coverage, other)? If these differ by applications, how do they differ? We welcome detailed Smart Grid network requirement analyses.

    RESPONSE: We view the Smart Grid as a series of interconnected, interoperable networks of control systems and asset-management tools, empowered by sensors, communication pathways and information tools – all designed to help utilities deliver energy more efficiently to customers. Smart Grid networks include (but are not limited to): substation automation, power distribution network monitoring & control, field operations communications, smart metering, and home area networks. Smart Grid networks must meet a range of demanding and immediate requirements: for security, coverage, functionality, reliability, performance, cost, and manageability (see table below). In addition, these networks must also offer architectures and technology roadmaps that extend well into the future, so this major utility investment can continue to support mission-critical operations into the next generation and beyond. A summary of differences in network requirements is as follows:

Network	Latency	Bandwidth	Security	Coverage	Endpoints
SCADA	Near real-time (milliseconds)	>2 Mpbs	Pervasive	>2 miles	Hundreds – thousands
Advanced Metering Infrastructure (AMI)	Seconds - minutes	< 2 Mbps	Pervasive	<2 miles	Hundreds of 1,000s – millions
Home Area Network	Seconds		Pervasive	Within home / office	Tens
Field Communications	Near real-tirne				Thousands

b. Which communications technologies and networks meet these requirements? Which are best suited for Smart Grid applications? If this varies by application, why does it vary and in what way? What are the relative costs and performance benefits of different communications technologies for different applications?

RESPONSE. There are more similarities than differences in the various Smart Grid network requirements. Implementing Smart Grid networks requires connecting existing utility grid infrastructure (some of it decades old), in order to leverage legacy investments, as well as enabling future innovations with adaptable "future-proof" investments in new Smart Grid technologies. We believe that all Smart Grid networks must possess the following characteristics:

- Smart Grid network solutions must be interoperable, scalable and flexible, and designed using widely-adopted standards, so that utilities benefit from a broader choice of vendors and lower costs associated with a competitive vendor ecosystem
- Smart Grid networks must possess the scalability, adaptability, remote programming and remote upgradeability to enable "future proofing" that anticipates and accommodates ongoing innovations in new technologies, services and capabilities
- Smart Grid networks must contain leading, standards-based security protocols and methods, and must be architected in 'granular' fashion, in order to rapidly identify, quarantine and isolate the network node or device that has been hacked, before it can cause further damage.

Standards-based technologies, specifically networks based on Ethernet and the Internet Protocol suite, provide a strategic foundation for Smart Grid networks. To reach millions of utility grid endpoints (e.g., meters, capacitor bank controllers, fault monitors, switches, video surveillance equipment, and distributed / micro generation equipment), and to ensure smooth integration with utility enterprise networks, a ubiquitous, Ethernet- and IP-based solution – such as what IEEE 802.16e - 2005, or WiMAX (Worldwide Interoperability for Microwave Access), delivers on many requirements for Smart Grid networks. WiMAX is the leading fourth-generation (4G) wireless broadband networking standard. It has been proven in hundreds of network deployments worldwide, and offers utilities a range of advantages over proprietary network communications solutions. For utilities, the WiMAX network offers the following key benefits:

1. **Commercial- / government-grade, end-to-end security** – provides the most secure, resilient, reliable standards-based protections against a wide range of network-level threats and attacks.
2. **High-performance, high-reliability, ubiquitous coverage** of the entire utility service area – with flexible deployment scenarios for rural, suburb and dense urban cores, and which enables integration of multiple utility Smart Grid applications onto a single communications network.
3. **Standards-based technology backed by an extensive world-class ecosystem** – WiMAX and the 500+ members of the WiMAX Forum (http://www.wimaxforum.org) are contributing billions of dollars of technology investments (and engineering resources) to enable a vendor ecosystem that offers mix-and-match, best-of-breed networking elements, ensures a vital supply chain for WiMAX network products and solutions.
4. **Secure connectivity to Smart Grid devices** – WiMAX employs leading, standards-based security protocols and methods for data transport and connectivity, including EAP-based authentication, AES-CCM-based authenticated encryption, and CMAC and HMAC based control message protection schemes
5. **Best of both worlds** – a WiMAX network offers utilities the security, stability, infrastructure, reliability and protection provided by public networks, which operate on government-licensed spectrum that insulates against unauthorized third-party access and use; as well as the benefits of virtual private networks, which include: optimal control, dedicated bandwidth, guaranteed service levels, and robust security.

PUBLIC NOTICE

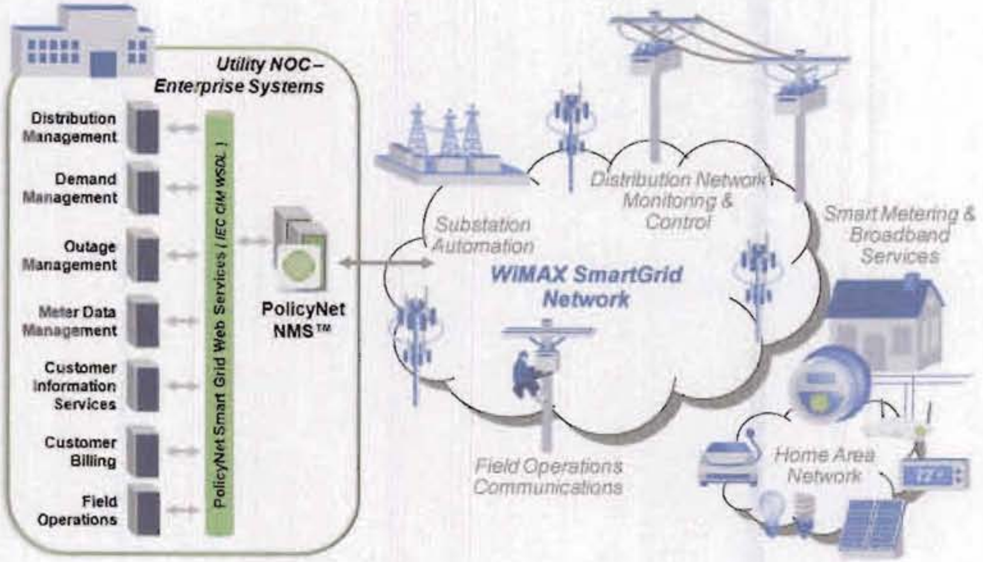
Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555



For additional information on WiMAX networking for utilities, please refer to the attached white paper, **WiMAX for Utilities**.

c. What types of network technologies are most commonly used in Smart Grid applications? We welcome detailed analysis of the costs, relative performance and benefits of alternative network technologies currently employed by existing Smart Grid deployments, including "last mile," backhaul and control network technologies.

   RESPONSE: Existing utility grid networks employ a variety of wireline and wireless network technologies, including (but not limited to): optical fiber, Ethernet, RF mesh, powerline communications (PLC). broadband over powerline (BPL), tower RF, and most recently, 4G cellular (e.g., WiMAX). Over many years, the electricity grid has been automated using these diverse networks (some of which connect to each other, some of which do not connect), the latest of which has been referred to as the "last mile" network of the Smart Grid – connecting, managing and automating electricity meters and associated services. There are a number of drawbacks to legacy networks:

   i. Lack of standards. Many legacy electricity grid networks (including metering networks) use proprietary network technologies, thus, utilities are limited to a specific vendor and its product development timeline, its bug-fix timeframes, its unique security schema, and the vendor's willingness (or unwillingness) to interoperate with other vendors' technologies.

ii. Increasingly unsuitable price / performance characteristics. As networks age, their maintenance and upkeep can become prohibitively expensive.
iii. Limited functionality and scale. As the Smart Grid emerges, its network technologies must manage the delivery of new forms of energy and new services. This is particularly important with innovations in metering. Many existing network technologies are unable to scale to accommodate these innovations; they lack either the bandwidth, or adequate control mechanisms, or both.
iv. Use of unlicensed spectrum. Grid networks which rely on unlicensed spectrum face many potential problems, including excessive crowding and interference, with no legal recourse for remedy. By contrast, licensed spectrum enables utilities to establish and maintain quality of service, guaranteed (and known) bandwidth, and therefore more predictable network performance.

d. Are current commercial communications networks adequate for deploying Smart Grid applications? If not, what are specific examples of the ways in which current networks are inadequate? How could current networks be improved to make them adequate, and at what cost? If this adequacy varies by application, why does it vary and in what way?

PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

RESPONSE. A quick review of competing last-mile Smart Grid network technologies is as follows:

Network Technology	Advantages	Disadvantages
RF mesh	• Resilient (due to node-to-node connectivity) • If a single node breaks down, multiple other routes are possible • Useful in 'delay tolerant' applications, such as meter reading	• Inherent latency (connectivity pathways are not always 'shortest path') • Potential scaling challenges, since peer-to-peer connectivity creates high network traffic 'overhead' • Usually proprietary technologies/protocols • Often on unlicensed spectrum

Powerline Carrier (PLC)	• Long distance
	  – Communicated wherever the wire goes
	• Demonstrated Scale: > 14 Million devices
	• Familiar to utilities (used in SCADA networks)
	• Control: leverages utility infrastructure & assets
	• Predictable: known feeder phase relationship / network path knowledge
		• Data performance
		  – 128bpd to 30bps
		  – Heat generation
		  – Message capacity
		• Limited / no security
		• Proprietary

Broadband Over PLC	• Proven with utilities
	  • Many SCADA and other Transmission Distribution network implementations
	• Control
	  • Leverages utility-controlled infrastructure
	• Standards (DLC)
	  • EN 50065 (CENELEC)
	  • IEC 61000-3
	  • FCC Part 15 Subpart
		• Performance at longer (e.g., WAN) distances, due to
		  • Noise, signal strength, operating frequency
		• Infrastructure costs
		  – Bridges required at all transformers
		  – Repeaters
		• Interference

4th Generation Wireless (e.g., WiMAX)	• Standards based, backed by a large vendor ecosystem • Standards based security • Licensed spectrum (e.g., quality of service) • Wireless technology: exceptionally flexible / resilient signal quality • All-IP network: lower infrastructure / maintenance costs	• Not yet widely deployed • Must obtain access to licensed spectrum from holders (e.g., Clearwire, etc.)

PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

e. How reliable are commercial wireless networks for carrying Smart Grid data (both in last-mile and backhaul applications)? Are commercial wireless networks suitable for critical electricity equipment control communications? How reliably can commercial wireless network transmit Smart Grid data during and after emergency events? What could be done to make commercial wireless networks more reliable for Smart Grid applications during such events? We welcome detailed comparisons of the reliability of commercial wireless networks and other types of networks for Smart Grid data transport.

RESPONSE. WiMAX commercial networks possess many important characteristics that comprise "reliability."

i. Leveraging FCC-licensed spectrum, WiMAX commercial networks can deliver specified service levels and quality of service. Utilities have the ability to negotiate specific service agreements that account for emergency and other mission-critical events.
ii. Standards and certification from the 500+ member WiMAX Forum, as well as a large number of participating vendors, from which utilities have greater choice of reliably certified technologies.
iii. Leading security methods and protocols. WiMAX networks incorporate leading security technologies, providing more reliable (and protected) network performance.

2. **Availability of Communications Networks**. Electric utilities offer near universal service, including in many geographies where no existing suitable communications networks currently exist (for last-mile, aggregation point data backhaul, and utility control systems). We seek to better understand the availability of existing communications networks, and how this availability may impact Smart Grid deployments.

a. What percentage of electric substations, other key control infrastructure, and potential Smart Grid communications nodes have no access to suitable communications networks? What constitutes suitable communications networks for different types of control infrastructure? We welcome detailed analyses of substation and control infrastructure connectivity, potential connectivity gaps, and the cost-benefit of different alternatives to close potential gaps.

b. What percentage of homes has no access to suitable communications networks for Smart Grid applications (either for last-mile, or aggregation point connectivity)?

c. In areas where suitable communications networks exist, are there other impediments preventing the use of these networks for Smart Grid communications?

d. How does the availability of a suitable broadband network (wireless, wireline or other) impact the cost of deploying Smart Grid application in a particular geographical area? In areas with no existing networks, is this a major barrier to Smart Grid deployment? We welcome detailed economic analyses showing how the presence (or lack) of existing communications networks impacts Smart Grid deployment costs.

RESPONSE to a-d:

i. Core benefits of WiMAX network technology include: flexibility in deployment, minimal equipment required and simplified deployment requirements. Several features contribute to its suitability across a variety of population densities, utility infrastructure and devices, and geographic locations:
   1. Centralized control / distributed intelligence. Use of WiMAX networks, in conjunction with software-based management of grid devices, can accommodate a diversity of grid topologies and requirements. For example, policy-based network management software architectures provide centralized management of software-enabled Smart Grid devices, providing for 'self healing' endpoints, while assuring cost-effective head-end control. Use of WiMAX networking with policy-based, software management of grid devices delivers exceptionally reliable, cost-effective Smart Grid network provisioning, management, and monitoring. For more information on policy-based networking, please refer to the attached white paper, **Policy-Based Network Management**.
   2. OFDMA / dynamic bandwidth allocation. The WiMAX 802.16e standard incorporates key features that enable exceptional flexibility in placement of both signal transmitter and receiver. For rural deployments, transmitters can be place further apart, for broader cell radius. In more dense urban cores, transmitters are placed closer together to ensure adequate capacity. In both instances the frequency modulation is automatically adjusted, to account for these differences (dynamic

bandwidth allocation). In addition, because the technology is designed for mobile applications (OFDMA), it's especially adept at making / maintaining challenging transmitter / receiver connections (OFDMA). Both of these features (and others) equate to cost-effective network planning / layout, deployment and operations. For more information on WiMAX networks, please refer to the attachment, **WiMAX Network Resource Management**.

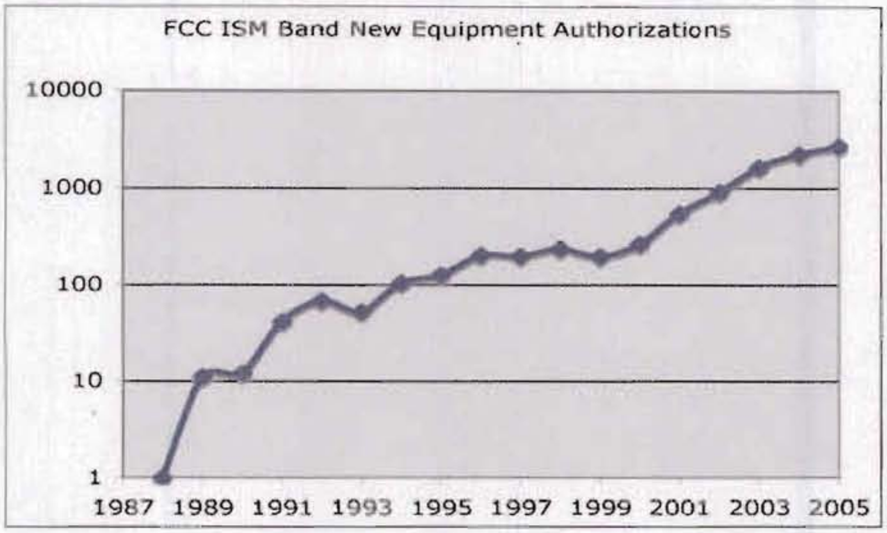
3. **Spectrum**. Currently, Smart Grid systems are deployed using a variety of communications technologies, including public and private wireless networks, using licensed and unlicensed spectrum. We week to better understand how wireless spectrum is or could be used for Smart Grid applications.
   a. How widely used is licensed spectrum for Smart Grid applications (utility-owned, leased, or vendor-operated)? For which applications is this spectrum used? We welcome detailed analyses of current licensed spectrum use in Smart Grid applications, including frequencies and channels.

   b. How widely used is unlicensed spectrum? For which applications is this spectrum used? We welcome detailed analyses of current unlicensed spectrum use in Smart Grid applications including frequencies and channels.

   c. Have wireless Smart Grid applications using unlicensed spectrum encountered interference problems? If so, what are the nature, frequency, and potential impact of these problems, and how have they been resolved?
   d. What techniques have been successfully used to overcome interference problems, particularly in unlicensed bands?

   e. Are current spectrum bands currently used by power utilities enough to meet the needs of Smart Grid communications? We welcome detailed analyses and discussion showing that the current spectrum is or is not sufficient.

   Response to 3a-3e: As mentioned above, licensed spectrum offers utilities clear, compelling benefits over unlicensed spectrum, including: greater control over network performance, and negotiated service levels and quality of service. At present, many proprietary Smart Grid network technologies leverage the 900 MHz spectrum. The chart below indicates that the ISM band (unlicensed spectrum) is growing ever more crowded. It is not feasible for utilities to compete with other users in unlicensed spectrum, as they will have no legal recourse to claim priority.



With regard to FCC discussions of "set asides" for utility-only spectrum, while that is theoretically an interesting possibility, the reality is more complex. Until and unless there are standards-based solutions provided by vendors for specific spectrum, this 'set aside' spectrum may not be immediately feasible or practical. That's because there is a delay between the time a technology standard is declared / agreed upon and an ecosystem of vendors has the resources (and time) to develop solutions that leverage these standards.

f. Is additional spectrum required for Smart Grid applications? If so, why are current wireless solutions inadequate?

   i. Coverage: What current and future nodes of the Smart Grid are not and will not be in the coverage area of commercial mobile operators or of existing utility-run connectivity required of each node not expected to be in coverage.

      RESPONSE: As mentioned above, WiMAX networks offer exceptionally flexible coverage scenarios, providing adequate options for a range of utility service areas.

   ii. Throughput: What is the expected throughput required by different communications nodes of the Smart Grid, today and in the future, and why will / won't commercial mobile networks and / or private utility-owned networks on existing spectrum be able to support such throughputs? We welcome detailed studies on the location and throughput requirements and characteristics of each communications node in the Smart Grid.

iii. Latency. What are the maximum latency limits for communications to / from different nodes of the Smart Grid for different applications, why will / won't commercial mobile networks be able to support such requirements, and how could private utility networks address the same challenge differently?

RESPONSE on Throughput and Latency. At present, throughput and latency requirements of last-mile Smart Grid networks are relatively lenient – for example, average meter reads equate to less than a single packet of data on a WiMAX network. And, if the meter fails to report a reading within a 6-hour window, it can always be captured in the next window. However, as new energy services are brought to market, both throughput and latency requirements will become more stringent. That's why Smart Grid networks must have enough bandwidth and scale to accommodate new forms of energy services, including time of use pricing, demand response, alternative energy transmission back into the grid, etc. Communicating and managing these services may provide more bandwidth-intensive. WiMAX offers up to 10 Mpbs – more than an order of magnitude greater than competing networks.

Security. What are the major security challenges, and the relative merits and deficiencies of private utility networks versus alternative solutions provided by commercial network providers, such as VPNs? Do the security requirements and the relative merits of commercial vs. private networks depend on the specific Smart Grid application? If so, how?

RESPONSE. System and network security are of critical concern for any large-scale, mission-critical network infrastructure. Since the Smart Grid is perhaps the most complex, mission-critical network of our time, utilities require Smart Grid technology that is secure, reliable, and self-healing. Specifically, to ensure adequate security, Smart Grid networks must architect security into all levels and layers – that is, to architect leading security into Smart Grid devices, into the data, into the Smart Grid network operating system software and services, and into the network transport mechanisms. Moreover, Smart Grid solution security architecture must support the cyber security principles of: confidentiality, integrity, availability, identification, authentication, access control, non-repudiation, secure operations, and auditing / accounting.

At present, many Smart Grid networks meet only some of the above security requirements. As an example (and by contrast), the GE WiMAX Smart Grid Solution is the first solution to leverage open, standards-based technologies to implement a WiMAX-compliant Smart Grid Solution (software + advanced metering) built for the WiMAX network. Moreover, its security architecture takes into account the risks associated with all aspects of Smart Grid network activity – including device power-up (or failure and re-energization) and identification, network entry and connectivity, data encryption and transport and Smart Grid network operations. To proactively anticipate points of vulnerability and mitigate risks, the GE WiMAX Smart Grid Solution incorporates leading standards-based security methodologies, protocols, and algorithms into Smart Grid devices, into device power-up and mutual authentication, authenticity validation, and authorization during Smart Grid network entry, into data encryption and integrity while in transit or at rest, and into Smart Grid network management, monitoring, and auditing. For more information on security, please refer to the attachment, **WiMAX Smart Grid Solution Security**.

iv. Coordination. Are there benefits or technical requirements to coordinate potential allocation of spectrum to the Smart Grid communications with other countries? What are they?

RESPONSE. With regard to the WiMAX 802.16e specification, the WiMAX Forum is coordinating the certification of WiMAX technologies with regard to specific spectrum bands. For more information, please refer to http://www.wimaxforum.org

v. Spectrum allocation. Are there any specific requirements associated with Smart Grid communications that require or rule out any specific band, duplexing scheme (e.g., FDD vs. RDD), channel width, or any other requirements or constraints?

RESPONSE. For spectrum requirements, please see answers provided above.

g. If spectrum were to be allocated for Smart Grid applications, how would this impact current, announced and planned Smart Grid deployments? How many solutions would use allocated spectrum vs. current solutions? Which Smart Grid applications would likely be most impacted?

RESPONSE. Please see response provided for Sections 3a – 3e.

4. **Real Time Data**. The Smart Grid promises to enable utility companies and their customers to reduce U.S. energy consumption using a variety of technologies and methods. Some of the most promising of these methods use demand response, in which utility companies can directly control loads within the home or business to better manage demand, or give price signals to encourage load shedding. Other methods reduce energy consumption simply by providing consumers access to their consumption information, via in-home displays, web portals, or other methods. Central to all of these techniques is energy consumption and pricing data.
   a. In current Smart Meter deployments, what percentage of customers has access to real-time consumption and / or pricing data? How is this access provided?
   b. What are the methods by which consumers can access this data (e.g., via Smart Meter, via a utility website, via third-party website, etc)? What are the relative merits and risks of each method?
   c. How should third-party application developers and device makers use this data? How can strong privacy and security requirements be satisfied without stifling innovation?
   d. What uses of real-time consumption and pricing data have been shown most effective at reducing peak load and total consumption? We welcome detailed analyses of the relative merits and risks of these methods.
   e. Are there benefits to providing consumers more granular consumption data? We welcome studies that examine how consumer or business behavior varies with the type and frequency of energy consumption data.
   f. What are the implications of opening real-time consumption data to consumers and the energy management devices and applications they choose to connect?

   RESPONSE to 4a – 4e. While we have no hard data or research to support our opinion, at present we believe that a tiny percentage of consumers currently have access to real time energy consumption information. That's because access to real-time consumption and pricing is just emerging with new technologies.

   We live in an Internet society, and thus believe that the most amenable means to provide consumers with real-time access to consumption and pricing is via web-based interfaces. This requires a smart meter that can safely, securely provide this real-time information via a web browser. The technology architecture to support this capability is as follows:
      i. Endow Smart Meters with a broadband switch router with Internet access.
      ii. Provide appropriate secure firewalls within the SmartMeter, to protect consumer privacy.
      iii. Provide intuitive web based user interfaces and displays of energy consumption information.

PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

---

iv. Provide software-based management of Smart Grid devices, along with a near real-time network connection, so that consumers can react to real-time information, and so that utilities can communicate new pricing programs and options in near real-time.

At present, we (Grid Net, GE, IBM and other vendors) are engaged in deploying a pilot study with a utility in Australia that will provide this infrastructure, and evaluate user behavior and response to real-time consumption and offers. The screenshot below is an illustration of the web-based interface used in the project.

PUBLIC NOTICE

Federal Communications Commission

445 12th St., S.W.

News Media Information 202 / 418-0500

Fax-On-Demand 202 / 418-2830

TTY 202 / 418-2555

5. **Home Area Networks**. We seek to understand the ways in which utilities, technology provides and consumers will connect appliances, thermostats, and energy displays to each other, to the electric meter, and to the Internet.
   a. Which types of devices (e.g., appliances, thermostats, an d energy displays, etc.) will be connected to Smart Meters? What types of networking technologies will be used? What type of data will be shared between Smart Meters and devices?
   b. Which types of devices (e.g., appliances, thermostats, an d energy displays, etc.) will be connected to the Internet? What types of networking technologies will be used? What types of data will be shared between these devices and the Internet?
   c. We welcome analyses that examine the role of broadband requirements for Home Area Networks that manage energy loads or deliver other energy management services.

   RESPONSE. There are many different ways in which vendors and utilities are responding to the challenges of Home Area Networks. As an example, please refer to the attachment, HAN Requirements. This is an early draft of a pilot project led by a utility in Australia, and includes participants, GE Energy, IBM, Grid Net and other technology providers. While requirements have been subsequently modified over the last six months, it serves as a useful example of the considerations involved in specifying a Home Area Network, including device selection / evaluation, networking technology, data collection and sharing, and more. This HAN pilot is expected to launch in early 2010.

WiMAX for Utilities: A White Paper

June 2009

340 Brannan Street, #500 San Francisco, CA 94107 t: 415.442.4623 f: 415.442.4628 www.grid-net.com

Executive Summary

The Smart Grid will likely be the most complex, mission-critical network build-out of the 21st century. Consequently, utilities need an industrial-strength, telecoms-grade communications network to serve as a secure, reliable and scalable foundation for their Advanced Metering Infrastructure (AMI) and Smart Grid architectures. The successful Smart Grid network must meet a range of demanding and immediate requirements, for security, coverage, functionality, reliability, performance, cost, and manageability. Just as critically, it must also offer an architecture and technology roadmap that extends well into the future, so this major utility investment can continue to support mission-critical operations into the next generation and beyond.

Trends in enterprise networking point to standards-based technologies, specifically to networks based on Ethernet and the Internet Protocol suite, for such a strategic foundation. To reach millions of utility field devices, and ensure smooth integration with the utility enterprise network, what's needed is a ubiquitous, Ethernet- and IP-based *wireless* solution – such as what IEEE 802.16, or WiMAX (Worldwide Interoperability for Microwave Access), delivers. WiMAX has emerged as the clear leader among fourth-generation (4G) wireless broadband systems, has been proven in hundreds of network deployments worldwide, and offers utilities a range of advantages over alternative collector-based and low-power RF mesh communications solutions.

A comprehensive consideration of Smart Grid requirements – especially security, performance, overall system cost (including ongoing operational costs); and a range of possible business models for network development (e.g., partnering with leading wireless carriers) – reveals that WiMAX is the leading networking technology for the Smart Grid.

For utilities, the WiMAX network offers the best of both worlds

- Security and reliability provided by government-licensed spectrum and network infrastructure that protect against unauthorized third-party bandwidth access and use
- Control, dedicated bandwidth, guaranteed service levels, and security of a virtual private network

WiMAX At a Glance

Mobile WiMAX (IEEE 802.16e-2005) was built from the ground up to be a cost-efficient, highly scalable wireless WAN platform for the support of mobile broadband data and real-time services (voice, video, gaming and other interactive applications). With an extensive ecosystem (more than 520 companies in the WiMAX Forum) and a growing number of deployments worldwide, WiMAX is being deployed ahead of competing 4G systems, delivering next-generation capabilities in time for major Smart Grid implementations.

Due to its efficient, adaptive use of bandwidth (spectrum), WiMAX is also an ideal technology for another class of network application, namely "machine-to-machine" (M2M) systems, in which Smart Grid devices (e.g., meters, capacitor bank controllers, fault monitors, switches, video surveillance equipment, and distributed / micro generation equipment) deployed over an extensive area are programmed and managed to automate the utility's enterprise systems' processes. Smart Grid infrastructure can run on a utility's own dedicated WiMAX network or be hosted on a commercial carrier's WiMAX service network as a managed "overlay" (or "Virtual Service") under agreed, utility-defined Service Level Agreements (SLAs).

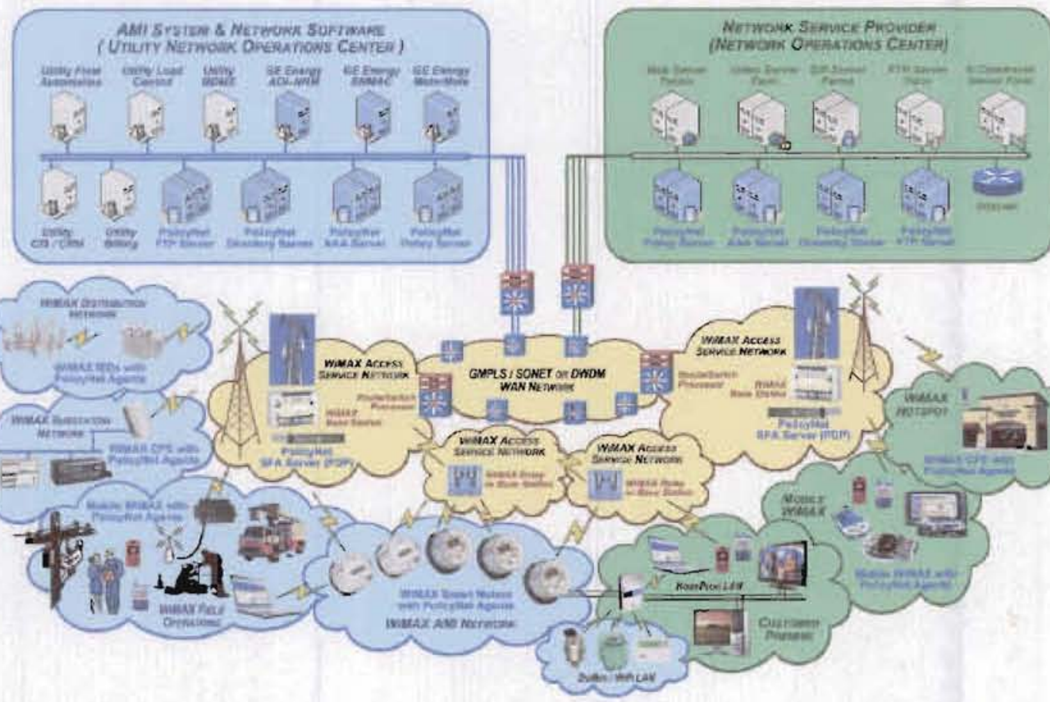


Figure 1 – WiMAX AMI and Retail Broadband – Total System Architecture

Benefits of WiMAX

Key benefits for utilities using WiMAX include:

1. **Commercial- / government-grade, end-to-end security** – provides the most secure, resilient, reliable standards-based protections against a wide range of network-level threats and attacks.
2. **High-performance, high-reliability, ubiquitous coverage** of the entire utility service area – with flexible deployment scenarios for rural, suburb and dense urban cores, and which enable integration of utility operations onto a single communications network.
3. **Standards-based technology backed by an extensive world-class ecosystem** – WiMAX and the 500+ members of the WiMAX Forum (http://www.wimaxforum.org) are contributing billons of dollars of technology investments (and engineering resources) to enable a vendor ecosystem that offers mix-and-match, best-of-breed networking elements, ensures a vital supply chain, and continuous innovation of transport, control, service and management platforms.
4. **Secure connectivity to "always-on" Smart Grid devices** – the right underlying architecture for Policy-Based AMI/ADI and Intelligent Grid control systems.
5. **Best of both worlds** – a WiMAX network offers utilities the security, stability, infrastructure, reliability and protection provided by public networks, which operate on government-licensed spectrum that insulates against unauthorized third-party access and use; as well as the benefits of virtual private networks, which include: optimal control, dedicated bandwidth, guaranteed service levels, and robust security.

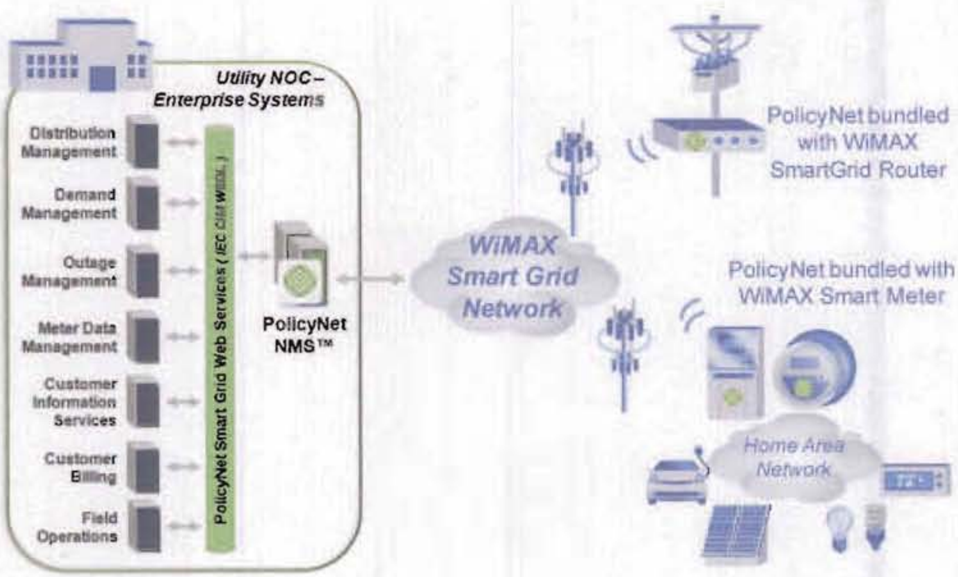


Figure 2 – WiMAX AMI/Smart Grid System Architecture

The WiMAX Access Service Network (ASN) provides a rich array of services, including dynamic security (PKIv2) and AAA support (EAP-TLS and EAP-RADIUS); "always-on" connectivity and instant outage alerts; Ethernet- and IP-level connectivity (VLAN, bridging and routing); a range of service qualities (QoS); and policy-based transactions, to support the entire range of utility applications.

WIMAX integrates seamlessly at Layer 2 (Ethernet, SONET, DWDM) and Layer 3 (IP) with existing and evolving enterprise / carrier (Local Loop and Core) networks.

For example, Grid Net's PolicyNet SmartGrid NMS software suite resides in the utility's control center, and reaches WiMAX Smart Meters and other endpoints via Core and Metro networks and finally, via the WiMAX ASN as shown in Figure 2 above. For more information on how PolicyNet implements policy-based networking and integrates with utility back-office applications, please refer to Grid Net's Policy-Based Networking white paper.

Detailed Review of WiMAX Benefits

1. WiMAX supports state-of-the art, government-grade device, user, and network security

As mentioned above, WiMAX provides superior, highly granular, end-to-end security, enabling utilities to identify, isolate and protect potentially compromised network nodes, and thereby protecting overall network security. As an example, the GE WiMAX SmartMeter uses a "Lifecycle" Approach to end-to-end security. During the assembly process in the factory, the GE WiMAX SmartMeter is provisioned with a unique pair of WiMAX Forum Certified x.509 Certificates, and it receives a unique "digital signature" that is created by using the Crypto EEPROM chipset on the board and the AES-CMAC hashing algorithm that is used post mutual authentication to verify the "authenticity" of the meter (i.e., verification that the meter board has no malicious software on board, and that the meter has not been otherwise physically tampered with after leaving the factory).

After a WiMAX SmartMeter is energized, it scans to find the WiMAX network and, after establishing a link layer connection with a base Station, undergoes an initial mutual authentication process via EAP/TLS with the PolicyNet SmartGrid NMS AAA (RADIUS) Server. Upon the successful completion of the mutual authentication process, the meter is granted authorized access to the WiMAX network and secure communications are established between the meter and the base station via the IEEE 802.16.e PKMv2 method.

Upon the successful mutual authentication process that enables the meter to gain secure access to the WiMAX network, the meter is provided a "quarantined" IP Address that only allows the meter to communicate with a "GateKeeper Process" that is in a non-routable subnet. The Gatekeeper Process uses a secondary tunneled challenge / response authentication method over TLS that requires the meter to generate its unique "digital signature" using the challenge key and the on-board Crypto EEPROM chip and the AES-CMAC hashing algorithm. If the meter generated digital signature matches the digital signature created in the factory, then the meter authenticity and meter firmware integrity are proven, and the meter is provided its Smart Grid x.509 Digital Certificate and private/public keys over the TLS connection. At this point, the meter is then provided with a Smart Grid IP Address, and the meter successfully establishes a mutually authenticated and secure connection to the Smart Grid Network (note: any subsequent configuration changes made to the meter, via the PolicyNet software, results in a "new" digital signature being dynamically generated and stored in the PolicyNet Secure Keystore – which is then used for subsequent authenticity validation processes). All subsequent communications between the meter and the PolicyNet software are performed over an encrypted COPS-PR/TLS connection established with the meter's Smart Grid x.509 Certificate and key pair.

2. WiMAX delivers superior technology for best service area coverage

As a sophisticated cellular technology, WiMAX was designed to reach end-user stations in the most demanding situations – even inside buildings. WiMAX features superior link budget, sophisticated use of multipath propagation, and other support for Non-Line-of-Sight (NLOS) communication. In licensed use, WiMAX is not limited by sub-watt RF power levels – using a number of techniques, such as sub-channelization and diversity, it can deliver the flexibility and resilience required to connect to WiMAX-enabled devices in otherwise hard-to-reach locations. For example, WiMAX-enabled Smart Meters, such as the GE WiMAX SmartMeter, mounted on residential exteriors will experience the highest possible rate of reach and coverage – a critical measure of AMI/Smart Grid program reliability.

WiMAX also features adaptive modulation techniques that allow it to deliver a wide range of service levels (mixes of bandwidth and quality of service) to a large number of users simultaneously. Consequently, a wide mix of traffic – from best-effort, small-scale data communications (e.g., meter reads, non-media-intensive web browsing, or routine operational control and data messages) to time-critical, high-bandwidth media streams and high-priority control signaling, can be supported routinely and easily on the same WiMAX network.

The "dynamic range" of a WiMAX network supports a wide assortment of services and devices. The network a utility installs to support AMI/Smart Grid can be extended to accommodate voice traffic – perhaps replacing land mobile radio with out-of-the-box Voice over IP (VoIP), video (e.g., substation security), or interactive multimedia (e.g., field-central office collaborative repairs of faulty equipment).

Due to its flexibility and capacity, WiMAX retail broadband wireless carriers (such as Clearwire in the USA and Unwired in Australia, who already offer retail WiMAX service in many utility service areas) are able to support M2M networking, and view utility AMI/Smart Grid projects as synergistic with their own network deployment and business plans.

2. WiMAX is an open industry standard backed by the WiMAX Forum, a world-class ecosystem

Unlike collector- and mesh-based AMI radio technologies, WiMAX is architected using open standards: it is completely free from proprietary content at every layer of its architecture. From the PHY and MAC layers through network architecture and management, WiMAX specifications are available from worldwide standards bodies (the IEEE, the IETF and the WiMAX Forum), enabling multiple WiMAX vendors to market interoperable silicon, software, base station and solution products into a fastgrowing, cost-competitive, vital marketplace. Consequently, utilities benefit from avoiding "vendor lock-in" while taking advantages of WiMAX attributes that include industry-leading network security, compelling supply chain economics, and a rapid innovation path for network lifecycle management. WiMAX differentiating features include:

Industry-leading network security: lessons learned from telecommunications and the Internet have proven that the only successful network security is standards-based network security. Leveraging the same communications and security protocols as the vast Internet/Ethernet community, and benefiting from the enormous pool of experience and expertise supplied by contributing members of the WiMAX forum organizations, ensure that WiMAX security innovations and improvements are exponentially greater than any single-vendor or proprietary technology (such as RF Mesh).

Favorable economics resulting from increased industry competition: the contributions of many industry players bringing innovation into the WiMAX market has driven the cost, variety and quality of products (chipsets, software, and base stations of different form factors, configurations, sizes, price levels, etc.) to the utility's advantage. In the last twelve months, WiMAX Forum member organizations have included new entrants in new tier-one equipment vendors, growth in tier-two players, acquisition of a tier-three by a tier-one vendor, and a steadily growing pool of technologies, platforms and features, i.e. in smart antennas, different frequency bands, multiple-network (WiFi-WiMAX) platforms, etc. In addition, WiMAX can be implemented as a flat IP network, delivering outstanding price / performance metrics, especially important for implementing cost-efficient yet high-performing and scalable Smart Grid networks.

Vibrant network lifecycle: as network build-out proceeds and new requirements emerge, a healthy vendor ecosystem fosters rapid, cost-effective innovation. For example, a variety of base station platforms – from multi-segment, macro base sites to omni, micro and pico sites – may be needed to provide the coverage required to serve the utility's service population: from very dense cells in the urban core, to average-density cells in suburban regions, to long-range solutions in rural areas. Since WiMAX platforms are interoperable, due to commitment to open standards and the WiMAX Forum's interoperability testing program, utilities can mix-and-match best-of-breed platforms from multiple vendors, as required.

3. WiMAX supports a resilient Smart Grid architecture

WiMAX is designed to support devices with powerful embedded intelligence and sophisticated behavior, such as the GE WiMAX SmartMeter and SmartGrid Router. The power of a WiMAX system comes from dynamic interactions between base station and Smart Grid devices, concerning the type and volume of data queued for transmission, the power level and modulation scheme for transceivers on each end of the connection, handover dynamics, quality of service requests, antenna parameters, etc. These settings are re-calculated and adjusted many times a second, for every device in the system, whether active or in "idle" mode – so that state changes happen quickly and smoothly, providing extremely efficient service for thousands and millions of devices throughout the Smart Grid network.

At higher layers in the communications network, this ability to support Smart Grid devices with complex state makes WiMAX superior to competing solutions as an AMI/Smart Grid infrastructure. For example, a Smart Meter has many state variables and parameters that, along with underlying WiMAX communications settings, may change over time and need to be tracked by a central management system in near real-time. These variables may include security, metering, configuration, control, monitoring, device health, diagnostics and fault, and firmware values and parameters. Dynamic encryption key management, meter usage and demand register values, baseline and Time of Use rate programs, Critical Peak Pricing state and values – the entire state space of a Smart Meter's ANSI C12.19 or IEC 62056 tables may all need to be shared between the device and the utility's AMI/Smart Grid system and related applications. Given these demanding requirements, waiting for a mesh routing table to converge, or for a pole-top mesh collector to finish polling another dozen meters, is unacceptable for Smart Grid reliability and performance.

As a full-featured telecommunications infrastructure, WiMAX implements the highest commercial-grade, end-to-end security subsystem, including mutual device-system and user-application authentication, service authorization, and billing-grade accounting, in order to support wireless carrier business transactions – from delivery of traffic at various levels of quality, to e-commerce, new service deployment, and advanced content delivery mechanisms. No collector- or mesh-based AMI system has this level of security support. By contrast, the Grid Net PolicyNet SmartGrid NMS suite takes full advantage of WiMAX's state-of the art security to deliver secure, reliable, scalable and high-performance WiMAX Smart Grid network management and monitoring.

(For more about the security features of WiMAX, please refer to the white paper, Policy-Based Networking, as well as to Grid Net's PolicyNet Security Guide.)

There are many other direct benefits of the WiMAX approach to AMI/Smart Grid architecture and implementation. As an example, its end-to-end, "smart client / stateful server" design allows for an efficient distribution of processing and decision enforcement, minimizing the required number of intermediate WiMAX devices and thereby reducing the points of network system vulnerability. By contrast, the amount and kind of state typically managed by a pole-top collector or within a mesh network simply doesn't occur in a WiMAX-based system. By building their Smart Grid networks using WiMAX, utilities can concentrate on managing and monitoring the performance of Smart Grid devices and central servers, with greater confidence in Smart Grid network reliability, availability and performance.

4. **WiMAX enables secure connectivity to "always-on" Smart Grid devices.** Unlike mesh network architectures, the GE WiMAX SmartMeter has a persistent network connection to the WiMAX network (maintained via Grid Net's PolicyNet software). For example, if there is an unscheduled removal of the meter (or it becomes un-energized, but with no outage condition), real-time tamper event messages are recorded in the meter's Event Log, and a tamper alarm is automatically generated by the PolicyNet Metering System and deployed via the WiMAX network. Leveraging the same technology used in the telecommunication industry to support network connection and service accounting for millions of concurrent users (e.g., policy-based networking), the PolicyNet